Chapter 21
Network Situational Awareness:
Sonification and Visualization in the Cyber Battlespace

Tom Fairfax
Security Risk Management, UK

Christopher Laing
Northumbria University, UK

Paul Vickers
Northumbria University, UK

ABSTRACT

This chapter treats computer networks as a cyber warfighting domain in which the maintenance of situational awareness is impaired by increasing traffic volumes and the lack of immediate sensory perception. Sonification (the use of non-speech audio for communicating information) is proposed as a viable means of monitoring a network in real time and a research agenda employing the sonification of a network's self-organized criticality within a context-aware affective computing scenario is given. The chapter views a computer network as a cyber battlespace with a particular operations spectrum and dynamics. Increasing network traffic volumes are interfering with the ability to present real-time intelligence about a network and so suggestions are made for how the context of a network might be used to help construct intelligent information infrastructures. Such a system would use affective computing principles to sonify emergent properties (such as self-organized criticality) of network traffic and behaviour to provide effective real-time situational awareness.

INTRODUCTION

This chapter explores some of the issues surrounding the problem of maintaining cyber situational awareness. Situational awareness is a term with its origins in military doctrine but has found its way into the mainstream and is especially applicable in the context of maintaining cyber security in computer networks. Networks are susceptible to a number of threats to their well-being from traffic congestion to deliberate attacks. In this chapter we show how the concept of cyber as a warfighting domain has traction and how applying a military understanding of the domain and situational awareness within it might help in finding new ways to maintain healthy networks. After

DOI: 10.4018/978-1-4666-6324-4.ch021

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

explaining the underlying concepts of the cyber operations spectrum and the dynamics underpinning it we show where situational awareness fits into this understanding. Next we explore how the projected growth network traffic volumes may make maintaining situational awareness increasingly challenging, especially as the cyber domain is intrinsically inaccessible to sensory perception which is traditionally needed for situational awareness. The limitations of current approaches to network visualization are touched upon and the possible role of using sonification for situational awareness activities is explored. Following this contextualization we then offer suggestions for potentially fruitful avenues of investigation that may yield big benefits in maintaining network situational awareness.

The principal objectives of this chapter are:

1. A presentation of computer networks as a cyber battlespace.
2. The role of situational awareness in this battlespace.
3. A critique of visualization approaches and the need to consider other modalities for the sensory perception of network behavior.
4. An agenda for future research based on sonification, self organized criticality, network context, and affective computing.

CYBERSPACE: THE NEW BATTLE SPACE?

There is significant debate in military circles about whether cyber has become the fifth warfighting domain. Traditional doctrine was directed towards operations on land and sea, and a combination of the two. History is well populated with examples of strategic operations combining operations on land supported by sea and vice versa. In the early 20th century, air was added as a third warfighting domain with increasing effect as a range of technologies have rapidly increased capability.

In the second half of the 20th century, space became the fourth warfighting domain and there is vigorous debate amongst practitioners and theorists about whether the cyber environment constitutes the fifth. There are a number of parallel lines of debate, however the central theme is focused on whether the cyber environment (sometimes known as cyberspace) is a discrete area of operations or whether it is a more pervasive concept that runs through all of the other domains.

Part of the principal challenge lies in the fact that whilst land, sea, air and space are physically distinct and are defined by similar criteria, cyberspace is defined in a different way, existing on an electronic plane rather than a physical and chemical one. Some would argue that cyber space is a vein which runs through the other four warfighting domains and exists as a common component rather than as a discrete domain. One can easily see how cyber operations can easily play a significant role in land, sea, air or space warfare, due to the technology employed in each of these domains.

On the other hand, this distinction is dependent on the way that we define the various domains. If our definitions are underpinned by a purely physical paradigm, then it is arguable that cyberspace is a very different type of context to the traditional warfighting domains. If, however, our definitions are based on an operational paradigm, then the distinction is less clear. It is possible to conduct entire operations in the cyber environment, made possible by the interconnected nature of the Internet and associated infrastructures. In the same way, it is common to have joint operations operating across multiple domains, including the cyber environment, and the cyber environment isn’t restricted to military warfighting scenarios.

A good example of a comprehensive cyber campaign occurred in April 2007, when Estonia was subjected to a wide range of concerted cyber attacks across a broad spectrum of government, commercial, industrial and media organizations. This sophisticated campaign effectively crippled

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/network-situational-awareness/115766

Related Content

An Approach for Hand Vein Representation and Indexing
D S. Guru, K B. Nagasundara, S Manjunathand R Dinesh (2011). *International Journal of Digital Crime and Forensics (pp. 1-15).*
www.irma-international.org/article/approach-hand-vein-representation-indexing/55499

European E-Signatures Solutions on the Basis of PKI Authentication Technology
Ioannis P. Chochliouros, Anastasia S. Spiliopoulou, Stergios P. Chochliourosand Konstantinos N. Voudouris (2009). *Socioeconomic and Legal Implications of Electronic Intrusion (pp. 290-304).*
www.irma-international.org/chapter/european-signatures-solutions-basis-pki/29371

Consequences of Corruption on Economy, Politics, and Society: The Case of India
Asim Kumar Karmakar, Priyanthi Bagchiand Somnath Karmakar (2023). *Theory and Practice of Illegitimate Finance (pp. 54-67).*
www.irma-international.org/chapter/consequences-of-corruption-on-economy-politics-and-society/330623

Task Offloading in Cloud-Edge Environments: A Deep-Reinforcement-Learning-Based Solution
Suzhen Wang, Yongchen Dengand Zhongbo Hu (2023). *International Journal of Digital Crime and Forensics (pp. 1-23).*
www.irma-international.org/article/task-offloading-in-cloud-edge-environments/332066

Future Cybercrimes in the Metaverse: A Comprehensive Forecast
Ibtesam Mohammed Alawadhi (2024). *Forecasting Cyber Crimes in the Age of the Metaverse (pp. 24-32).*
www.irma-international.org/chapter/future-cybercrimes-in-the-metaverse/334493